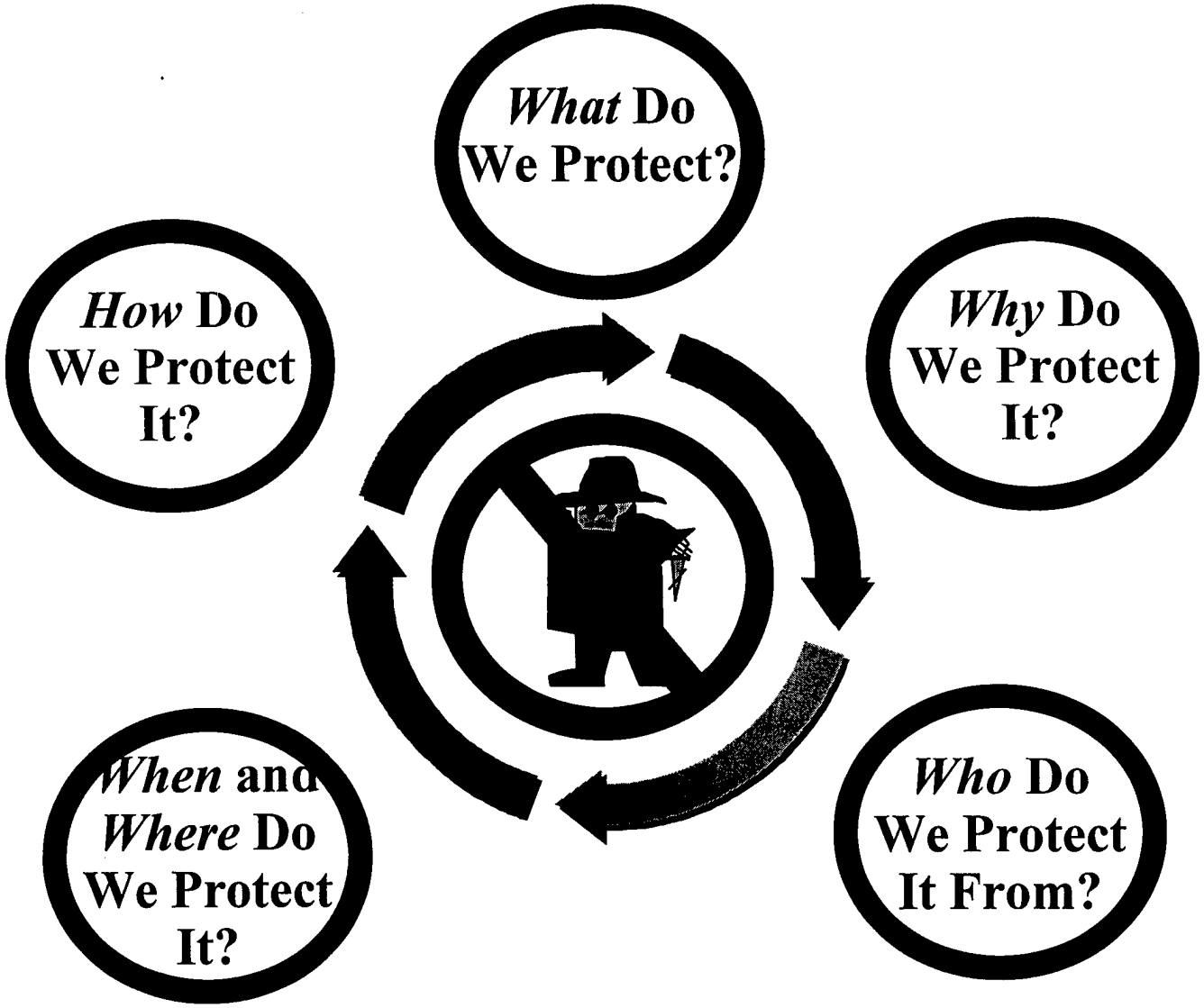
Program Protection Planning in the USAF TENCAP Program

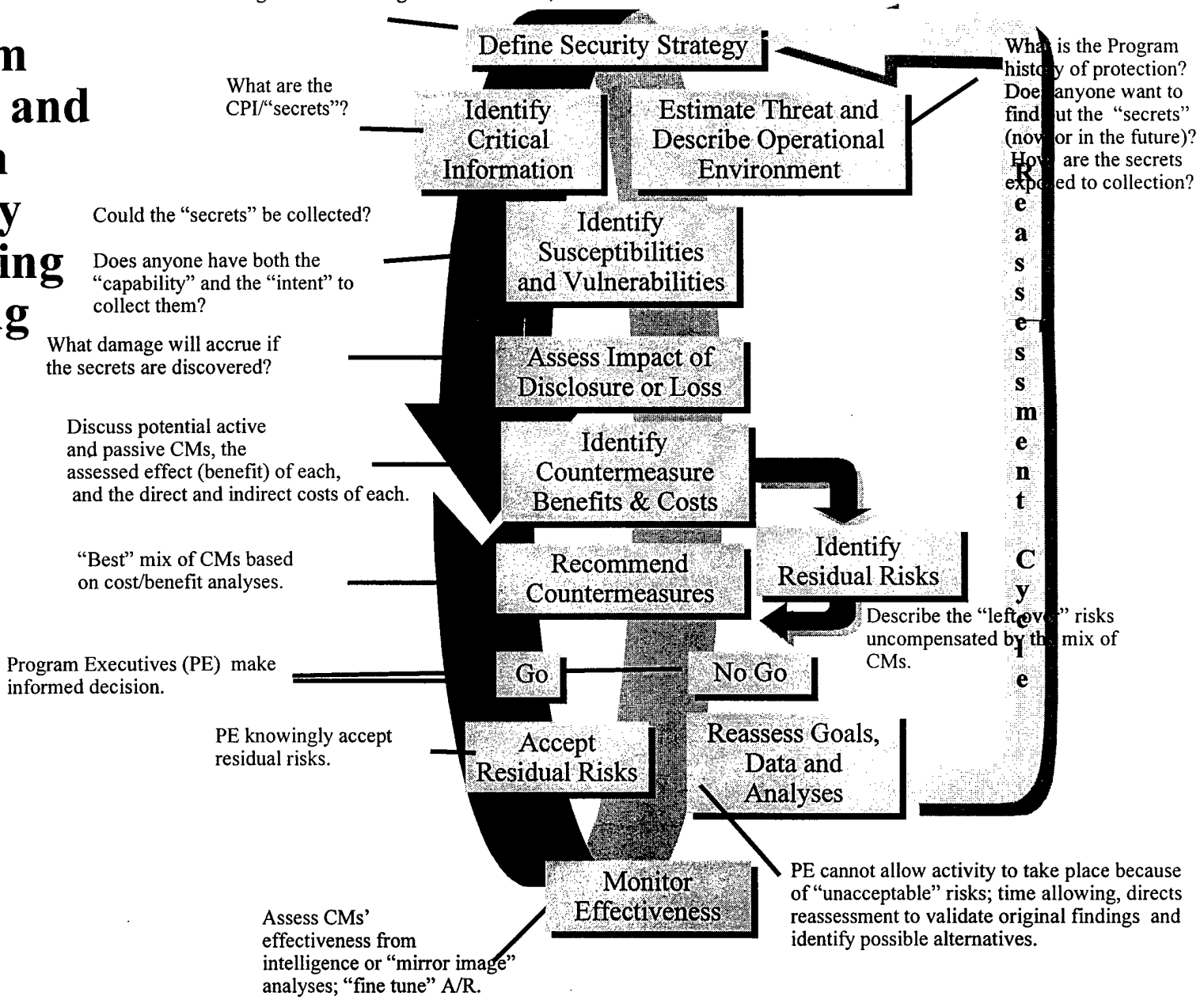
A Real-World Application of Risk Management to Contain Security Costs©

Aegis Research Corporation

©Howard B. Low 1998
Aegis Research Corporation, Space Engineering Center
1551 Vapor Trail, Colorado Springs, CO 80916
(719) 570-7041/567-9946 Fax (719) 570-7689/567-9898
E-mail: hblow@pcisys.net, lowhowab@fafb.af.mil



Program Protection and System Security Engineering Planning Cycle



Development of Security Engineering Curricula at US Universities

Session IV: Technology and Policy Focus Groups

Mary Lynn Garcia
Sandia National Laboratories
PO Box 5800 – 0762
Albuquerque, NM 87185-0762
(505)-844-2010
FAX: (505)-844-2193
mtgarci@sandia.gov

Development of Security Engineering Curricula at US Universities

Abstract

The Southwest Surety Institute was formed in June, 1996 by Arizona State University (ASU), New Mexico Institute of Mining and Technology (NM Tech), New Mexico State University (NMSU), and Sandia National Laboratories (SNL) to provide new educational programs in Security Engineering. This is the first science-based program of its kind in the United States, directed at educating Security Engineers to help government and industry address their security needs. Current courses include security system design, evaluation, principles and technology, the criminal justice system, and explosives surety.

Each member brings a unique educational capability to the Institute. NMSU provides a Security Technology minor, merging programs in Criminal Justice and Engineering Technology. NM Tech has a formidable explosives testing and evaluation facility. ASU is developing a Masters program in Security Engineering at their School of Technology located on a new campus in Mesa, Arizona. The Sandia National Laboratories security system design and evaluation process forms the basis for the Security Engineering curricula. In an effort to leverage the special capabilities of each university, distance education will be used to share courses among Institute members and eventually with other sites across the country.

The Institute will also pursue research and development funding in the areas of physical security, information security, computer modeling and analysis, and counterterrorist technology. Individual Institute members are currently working with sponsors from government and industry in areas such as counterterrorism, microelectronics, banking, aviation, and sensor development.

Introduction

The protection of critical assets has always been an important and difficult task. With the emergence of new threats including weapons of mass destruction, domestic terrorism, narcotics trafficking, international crime, and information warfare (1), this task has attracted more attention in both government and industry. At the same time, a heightened awareness has developed among the US public about the risks associated with high visibility targets. The World Trade center, Oklahoma City, and the Atlanta Olympics bombing are tragic evidence of the increased susceptibility felt by American citizens. This increased exposure leads to the realization that these risks and their consequences must be mitigated in order to assure the safety of our citizens as much as possible. Every day we are reminded of our susceptibility to attack. These attacks may be physical, electronic, or financial.

As in any other discipline, security requires the understanding and application of standard principles and concepts in order to achieve effective and consistent solutions. Today, the security industry is very fragmented, with no entry barriers. There is no system of accepted methodologies, basic principles, standard tools and tests, or universally accepted definitions. While security consultants can offer useful and pertinent services to their private industry and government customers, their effectiveness can be diminished due to the lack of grounding in common principles or an understanding of systems concepts. In all other professional fields there are unifying principles, basic concepts, and accepted definitions - in physics, electrical engineering, criminal justice, accounting, and medicine. Yet, in a field where researchers estimate the total cost of crime to be $425 billion each year, including $45 billion in property losses; and a $65 billion private security industry (2), there are no such unifying principles. The security professional of the future will be required to have a good understanding of technology, legal issues, and business practices to effectively protect people, property and information. By establishing educational programs that teach the common approaches, principles, and definitions, our universities and colleges can help bring necessary order and structure to this vital area.

Recognition of this problem inspired the creation of the Southwest Surety Institute (SSI) in 1996. Founding members Arizona State University- East (ASUE), New Mexico Institute for Mining and Technology (NM Tech), New Mexico State University (NMSU) and Sandia National Laboratories (SNL) were joined by Louisiana State University (LSU) in January, 1998. Programs in security engineering technology have been established at each university to provide unique, science-based curricula to students.

The discipline of security engineering will incorporate principles of business, technology, and criminal justice to educate a new generation of security engineers and managers who will be better able to make decisions as to when and how to protect assets. This science will also clarify the differences between safety and security, thereby adding some additional precision to security practices. Briefly, safety systems are needed to protect people and assets from abnormal environments, such as fire, earthquake, or electrical

faults. Security systems, on the other hand, are meant to protect people and assets from attack by malevolent individuals or groups.

Program descriptions

The various members of the SSI currently offer three programs. New Mexico State University, located in Las Cruces, NM has created a security technology minor through the merging of select courses from the Criminal Justice and Engineering Technology departments. Students from each department take basic courses offered by the other department and then finish out the minor by taking a capstone course in security technology, where students are taught a design methodology and approach and learn the proper application of security technologies to balanced security systems. NMSU is planning on adding additional courses and upgrading the minor to a supplemental major. Table 1 shows a brief summary of courses available to students enrolled in the minor at NMSU.

Minor requirements for all students:	
CJ 101	Introduction to Criminal Justice
CJ 412	Introduction to Security Technology and Loss Prevention
ET 407	Security Technology
Additional requirements for Criminal Justice students:	
ET 307	Principles of Technology I
ET 357	Principles of Technology II
	One elective in Criminal Justice
Additional requirements for Engineering Technology students:	
CJ	3 electives in Criminal Justice OR 2 electives in Criminal Justice AND
CHEM 540	Explosives Surety (distance education delivery from NM Tech)

Table 1 - New Mexico State University - Minor Program in Security Technology

Arizona State University - East is creating a Masters program in Security Engineering Technology that will begin in the fall of 1998 at their School of Technology, located on a new campus in Mesa, Arizona. The degree is open to graduates of appropriate programs in engineering and engineering technology, as well as graduates of traditional criminal

justice programs who have an acceptable technical background. This includes graduates of the programs at schools belonging to the Southwest Surety Institute. The program is designed to be completed in three semesters and one summer. Students will begin the course of study in the fall, with a target graduation by the end of the following summer. The program will include nine courses and an applied project, resulting in a total of 32 semester credit hours. The details of the courses and program of study are shown in Table 2.

Fall Semester	**CH**	***Winter Session***	**CH**	***Spring Semester***	**CH**
MET 510 Res Meth in Eng Tech	3	SET 594 Applied Project	2	SET 500 Security Law/ Regulation	3
MET 540 Econ Anal of Engineering Systems	3			SET 540 Risk Analysis/ Decision Making	3
SET 560 Physical Security Sys I	3			SET 561 Physical Security SysII	3
SET 570 Instrmntn Systems	3			SET 580 Forensic Technology	3
Totals	*12*		*2*		*12*
Summer Session					
SET 581 Computer Fraud	3				
SET 594 Applied Project	3				
Total	*6*				
Program total	**32**				

Table 2- ASU Master's Program in Security Engineering Technology - Sample Curriculum

In addition to the program described above, there will be a need to provide a set of normalization courses for those interested and otherwise qualified baccalaureate degree students with backgrounds that are lacking the technical basis necessary for the proposed program of study. It is possible for a motivated and mature student to obtain this framework in two semesters, if the student has a reasonable background in science and mathematics, such as provided by a typical liberal arts education. The normalization sequence may be completed at any member institution of the Southwest Surety Institute. These normalization courses may be taken at the students' current university or at ASU. This structure will support the use of a starting class every Fall at ASU, with graduation from the program at the end of the following summer, assuming the student attends full time.

NM Tech and LSU have enhanced their existing resources and capabilities to develop a counterterrorism education program. NM Tech operates the Energetic Materials Research and Testing Center (EMRTC), which has counterterrorism research facilities and programs already in place. LSU trains approximately 15,000 first responders each year, through its Anti-Terrorist Training Assistance Program and Fire and Emergency Training Institute. The two universities have recently joined together to provide training to international law enforcement agencies, conducted cooperatively at both schools. The Academy for Counterterrorism Education (ACE) was developed in response to the growing threat of terrorist acts on US military forces and civilian populations. Terrorist bombings such as the Khobar Towers in Saudi Arabia and in Oklahoma City demonstrate this alarming threat. While the US is spending millions of dollars on counterterrorism and force protection technology, state and local first responders are unprepared to deal with large explosive devices and weapons of mass destruction. Federal, military, National Guard, state and local police, fire, medical, and other first responders need training to prevent, detect, and respond to terrorist attacks.

The goal of ACE is to provide first responders with counterterrorism training. ACE will conduct a series of short courses and seminars at NM Tech, LSU, and selected locations throughout the US. Planned courses of instruction include Emergency Response Managers and Commanders Seminar (3 days), Chem/Bio/Explosives Responder Trainers (5 days) and a Large Explosive Device Post-Blast Analysis Course (5 days). Other planned educational support activities include "take-home" training and specialized equipment packages, an on-line distance education resource center, and graduate assistance and internships to expand the domestic base of expertise. For current updates on ACE, visit their homepage at *www.emrtc.nmt.edu/ace/.*

Individually, both NM Tech and LSU are also developing programs incorporating security engineering curricula. NM Tech is implementing an option (minor) program that will include courses in shock physics, explosives chemistry, explosives engineering, and security technology. In addition, students enrolled in doctoral programs in science and engineering may add these courses to their program of study and increase their knowledge of security concepts. In support of the Southwest Surety Institute educational goals and to exploit the unique capabilities offered by NM Tech, Explosives Surety Chemical Engineering 489, is currently offered via distance learning to NMSU and SNL; the course is expected to be offered at ASU as part of the MS program.

LSU is planning on an initial offering of a one week course entitled Design and Evaluation Process for Physical Security Systems in July of 1998 and will develop additional courses to supplement this program over time. The one week course, taught by experts from Sandia National Laboratories, will be repeated twice each year in the New Orleans area as part of the LSU continuing education program. These offerings allow access to the education and training programs of the Institute for those interested in continuing professional education or refresher training, such as law enforcement or industrial security managers.

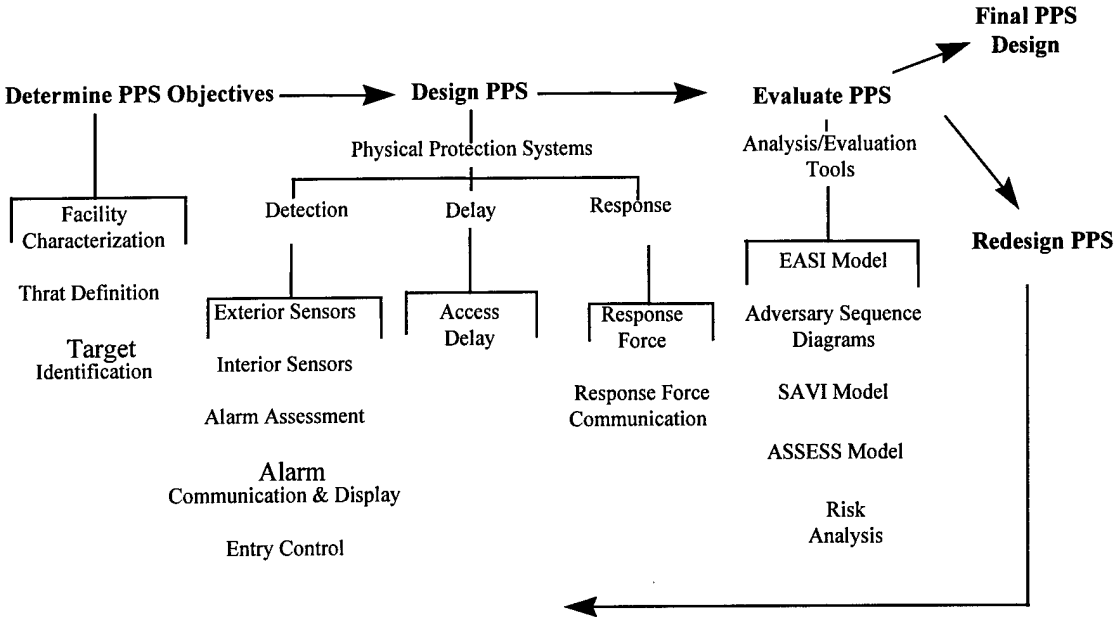


Fig. 1 – Sandia Design and Evaluation Process Outline

All of the programs will bring together engineering, business and criminal justice elements in order to create a new generation of security engineers and managers who will be better prepared to effectively achieve the security goals of their organizations. These programs are based on the design and evaluation methodology developed at SNL over the past 25 years. An outline of the approach is shown in Figure 1. This approach integrates people, procedures and equipment into a balanced and effective system that protects targets from the identified threat. The process is dependent on the use of performance measures, so that security professionals and their business managers will have a way of identifying what improvements they will achieve by performing proposed upgrades. A major benefit of these educational programs will be the capability of graduates to effectively use existing computer analysis models to predict the performance of a security system using such performance measures as probability of detection, delay times, response force times, probability of communication and assessment, and probability of interruption or neutralization.

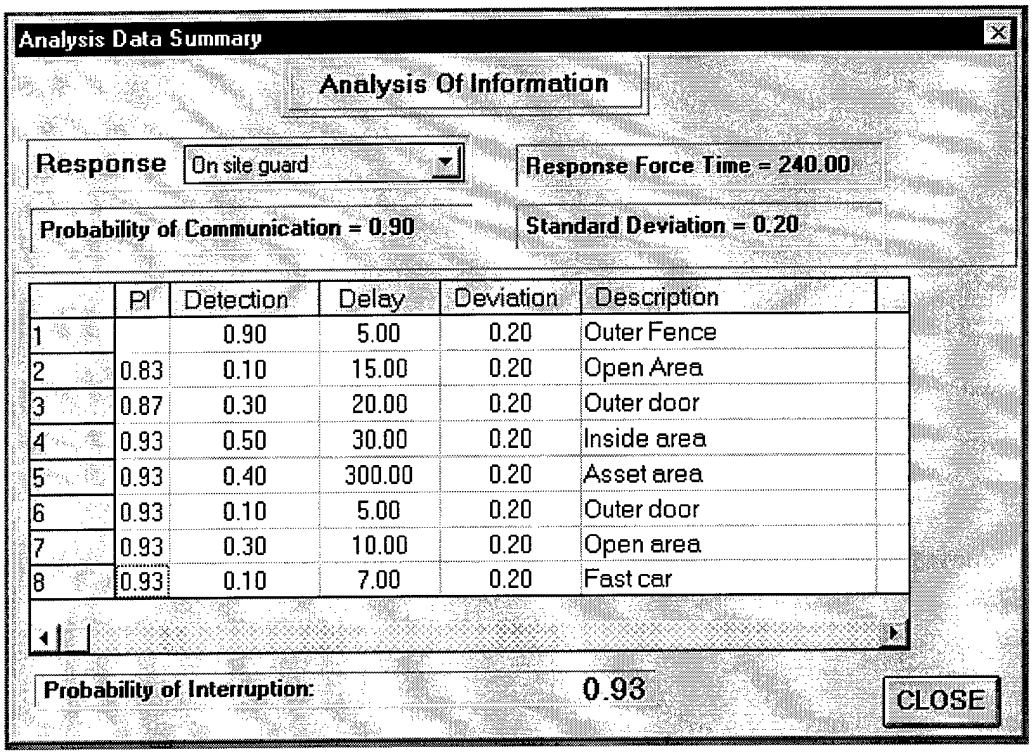
In an effort to leverage the special capabilities of each university, distance education will be used to share courses among Institute members and eventually with other sites across the country. A grant of $2 million dollars from the US government will provide the initial funding required to establish the various programs.

Benefits/Future path

Perhaps the greatest need in the field of security today is in analysis of systems, i.e., predicting when enough has been done to meet the system objectives. This can be accomplished through the use of models already developed by the Department of Energy that incorporate performance measures as inputs and produce probabilities of success as

the output. The unique aspect of these programs is centered on analyzing proposed security system designs or upgrades to help determine if the change is cost effective

An example of these analytic results is shown in Figure 2. If we assume that an intruder has entered a facility by climbing a fence, crossing an inner area, defeating a door, stealing the target, then exiting the facility, the result of a typical analysis can be seen. We can use the probability of interruption to predict whether the response force will arrive at the target or boundary in enough time to interrupt the adversary.



	PI	Detection	Delay	Deviation	Description
1		0.90	5.00	0.20	Outer Fence
2	0.83	0.10	15.00	0.20	Open Area
3	0.87	0.30	20.00	0.20	Outer door
4	0.93	0.50	30.00	0.20	Inside area
5	0.93	0.40	300.00	0.20	Asset area
6	0.93	0.10	5.00	0.20	Outer door
7	0.93	0.30	10.00	0.20	Open area
8	0.93	0.10	7.00	0.20	Fast car

Figure 2 - Adversary Path Analysis

Through the use of performance measures, graduates of these programs will have the knowledge to first determine the security objectives of the system, design the proper mix of detection, delay and response technologies to meet the objectives, and then analyze proposed additions or upgrades. This capability will lead to enhanced communication within the security community and reinforce efforts to provide useful and effective systems. The increase in system performance can then be used to make an informed decision, before the actual implementation of the system, as to the adequacy of the proposed changes. This will provide a rationale for any expenditure, as well as a measure of expected system performance, which can then be used to mitigate the risk of loss of the asset. Justification of the cost compared to improved performance will enable the enterprise to make good decisions on where to spend limited dollars.

As the programs grow and develop, existing tools and approaches will be modified and improved to create tools useful to all segments of the government and private industry, across the entire spectrum of protection requirements, from lowest to highest. These include development of new technologies to detect and assess causes of alarms, integration of technology into effective sub-systems, creation of new unclassified databases for use in computer models, and creation of new computer models to allow for validated predictions of security system performance. Applications in physical security, information security, computer modeling and analysis, and counterterrorist technology form the core of future research and development proposals by institute members.

This new generation of security professionals will posses the training and knowledge to test components, determine required performance measures, fit security objectives into the larger goals of the enterprise, provide information to management to help make investment decisions, and lessen risk to the enterprise by understanding the level of protection offered by the security system.

Summary

The Southwest Surety Institute was formed in 1996 to create unique, science-based educational programs in security engineering. The programs will integrate business, technology, and criminal justice elements to educate a new generation of security professionals. Graduates of the programs will better understand basic security system design and evaluation and contribute to strengthening of the body of knowledge in the area of security. A systematic approach incorporating people, procedures, and equipment will be taught that will emphasize basic security principles and establish the science of security engineering. The use of performance measures in the analysis of designed systems will enable effective decisions by an enterprise and provide the rationale for investment in security systems.

Along with educational programs, Institute members will conduct original research and development built on existing relationships with sponsors from government and industry in areas such as counterterrorism, microelectronics, banking, aviation, and sensor development. Additional information and updates on the Southwest Surety Institute are available via the Institute home page at *www.emrtc.nmt.edu/ssi.*

References:

1. "Summer blockbuster: Assessing the real threat," Boston Globe, August 20, 1997
2. "The Economics of Crime," Business Week, December 13,1993, pp. 72-81